

**EXHIBIT C**



FEDERAL TRADE COMMISSION  
CONSUMER ADVICE

Article

## What To Know About Cryptocurrency and Scams

---

Confused about cryptocurrencies, like bitcoin or Ether (associated with Ethereum)? You're not alone. Before you use or invest in cryptocurrency, know what makes it different from cash and other payment methods, and how to spot cryptocurrency scams or detect cryptocurrency accounts that may be compromised.

[What To Know About Cryptocurrency](#)

---

[Paying With Cryptocurrency?](#)

---

[How To Avoid Cryptocurrency Scams](#)

---

[How To Report Cryptocurrency Scams](#)

## What To Know About Cryptocurrency

### What is cryptocurrency?

Cryptocurrency is a type of digital currency that generally exists only electronically. You usually use your phone, computer, or a cryptocurrency ATM to buy cryptocurrency. Bitcoin and Ether are well-known cryptocurrencies, but there are many different cryptocurrencies, and new ones keep being created.



## How do people use cryptocurrency?

People use cryptocurrency for many reasons — quick payments, to avoid transaction fees that traditional banks charge, or because it offers some anonymity. Others hold cryptocurrency as an investment, hoping the value goes up.

## How do you get cryptocurrency?

You can buy cryptocurrency through an exchange, an app, a website, or a cryptocurrency ATM. Some people earn cryptocurrency through a complex process called “mining,” which requires advanced computer equipment to solve highly complicated math puzzles.

## Where and how do you store cryptocurrency?

Cryptocurrency is stored in a digital wallet, which can be online, on your computer, or on an external hard drive. A digital wallet has a wallet address, which is usually a long string of numbers and letters. If something happens to your wallet or your cryptocurrency funds — like your online exchange platform goes out of business, you send cryptocurrency to the wrong person, you lose the password to your digital wallet, or your digital wallet is stolen or compromised — you’re likely to find that no one can step in to help you recover your funds.

## How is cryptocurrency different from U.S. Dollars?

Because cryptocurrency exists only online, there are important differences between cryptocurrency and traditional currency, like U.S. dollars.

- **Cryptocurrency accounts are not backed by a government.** Cryptocurrency held in accounts is **not** insured by a government like U.S. dollars deposited into an FDIC insured bank account. If something happens to your account or cryptocurrency funds — for example, the company that provides storage for your wallet goes out of business or is hacked — the government has no obligation to step in and help get your money back.
- **Cryptocurrency values change constantly.** The value of a cryptocurrency can change rapidly, even changing by the hour. And the amount of the change can be significant. It depends on many factors, including supply and demand. Cryptocurrencies tend to be more volatile than more traditional investments, such as stocks and bonds. An investment that's worth thousands of dollars today might be worth only hundreds tomorrow. And, if the value goes down, there's no guarantee it will go up again.

## Paying With Cryptocurrency?

There are many ways that paying with cryptocurrency is different from paying with a credit card or other traditional payment methods.

- **Cryptocurrency payments do not come with legal protections.** Credit cards and debit cards have [legal protections](#) if something goes wrong. For example, if you need to [dispute a purchase](#), your credit card company has a process to help you get your money back. Cryptocurrencies typically do not come with any such protections.
- **Cryptocurrency payments typically are not reversible.** Once you pay with cryptocurrency, you can usually only get your money back if the person you paid sends it back. Before you buy something with cryptocurrency, know the seller's reputation, by doing some research before you pay.
- **Some information about your transactions will likely be public.** People talk about cryptocurrency transactions as anonymous. But the truth is not that simple. Cryptocurrency transactions will typically be recorded on a public ledger, called a "blockchain." That's a public list of every cryptocurrency transaction — both on the payment and receipt sides. Depending on the blockchain, the information added to the blockchain can include details like the transaction amount, as well as the sender's and recipient's wallet addresses. It's sometimes possible to use transaction and wallet information to identify the people involved in a specific transaction. And when you buy something from a seller who collects other information about you, like a shipping address, that information can also be used to identify you later on.

## How To Avoid Cryptocurrency Scams

Scammers are always finding new ways to steal your money using cryptocurrency. To steer clear of a crypto con, here are some things to know.

- **Only scammers demand payment in cryptocurrency.** No legitimate business is going to demand you send cryptocurrency in advance – not to buy something, and not to protect your money. That's always a scam.
- **Only scammers will guarantee profits or big returns.** Don't trust people who promise you can quickly and easily make money in the crypto markets.
- **Never mix online dating and investment advice.** If you meet someone on a dating site or app, and they want to show you how to invest in crypto, or asks you to send them crypto, that's a scam.

### Spot crypto-related scams

Scammers are using some tried and true scam tactics — only now they're demanding payment in cryptocurrency. Investment scams are one of the top ways scammers trick you into buying cryptocurrency and sending it on to scammers. But scammers are also impersonating businesses, government agencies, and a love interest, among other tactics.

### Investment scams

Investment scams often promise you can "make lots of money" with "zero risk," and often start on social media or online dating apps or sites. These scams can, of course, start with an unexpected text, email, or call, too. And, with investment scams, crypto is central in two ways: it can be both the investment and the payment.

Here are some common investment scams, and how to spot them.

- **A so-called "investment manager" contacts you out of the blue.** They promise to grow your money — but only if you buy cryptocurrency and transfer it into their online account. The investment website they steer you to looks real, but it's really fake, and so are their promises. If you log in to your "investment account," you won't be able to withdraw your money at all, or only if you pay high fees.
- **A scammer pretends to be a celebrity who can multiply any cryptocurrency you send them.** But celebrities aren't contacting you through social media. It's a scammer. And if you click on an unexpected link they send or send cryptocurrency to a so-called celebrity's QR code, that money will go straight to a scammer and it'll be gone.
- **An online "love interest" wants you to send money or cryptocurrency to help you invest.** That's a scam. As soon as someone you meet on a dating site or app asks you for money, or offers you

investment advice, know this: that's a scammer. The advice and offers to help you invest in cryptocurrency are nothing but scams. If you send them crypto, or money of any kind, it'll be gone, and you typically won't get it back.

- **Scammers guarantee that you'll make money or promise big payouts with guaranteed returns.** Nobody can make those guarantees. Much less in a short time. And there's nothing "low risk" about cryptocurrency investments. So: if a company or person promises you'll make a profit, that's a scam. Even if there's a celebrity endorsement or testimonials from happy investors. Those are easily faked.
- **Scammers promise free money.** They'll promise free cash or cryptocurrency, but free money promises are always fake.
- **Scammers make big claims without details or explanations.** No matter what the investment, find out how it works and ask questions about where your money is going. Honest investment managers or advisors want to share that information and will back it up with details.

Before you invest in crypto, search online for the name of the company or person and the cryptocurrency name, plus words like "review," "scam," or "complaint." See what others are saying. And read more about other common [investment scams](#).

### Business, government, and job impersonators

In a business, government, or job impersonator scam, the scammer pretends to be someone you trust to convince you to send them money by buying and sending cryptocurrency.

- **Scammers impersonate well-known companies.** These come in waves, and scammers might say they're from Amazon, Microsoft, FedEx, your bank, or many others. They'll text, call, email, or send messages on social media — or maybe put a pop-up alert on your computer. They might say there's fraud on your account, or your money is at risk — and to fix it, you need to buy crypto and send it to them. But that's a scam. If you click the link in any message, answer the call, or call back the number on the pop-up, you'll be connected to a scammer.
- **Scammers impersonate new or established businesses offering fraudulent crypto coins or tokens.** They'll say the company is entering the crypto world by issuing their own coin or token. They might create social media ads, news articles or a slick website to back it all up and trick people into buying. But these crypto coins and tokens are a scam that ends up stealing money from the people who buy them. Research online to find out whether a company has issued a coin or token. It will be widely reported in established media if it is true.
- **Scammers impersonate government agencies, law enforcement, or utility companies.** They might say there's a legal problem, that you owe money, or your accounts or benefits are frozen as part of an investigation. They tell you to solve the problem or protect your money by buying

cryptocurrency. They might say to send it to a wallet address they give you — for “safe keeping.” Some scammers even stay on the phone with you as they direct you to a cryptocurrency ATM and give step-by-step instruction on how to insert money and convert it to cryptocurrency. They’ll direct you to send the crypto by scanning a QR code they give you, which directs the payment right into their digital wallet — and then it’s gone.

- **Scammers list fake jobs on job sites.** They might even send unsolicited job offers related to crypto like jobs helping recruit investors, selling or mining cryptocurrency, or helping convert cash to crypto. But these so-called “jobs” only start if you pay a fee in cryptocurrency. Which is always a scam, every time. As your first task in your “job,” these scammers send you a check to deposit into your bank account. (That check will turn out to be fake.) They’ll tell you to withdraw some of that money, buy cryptocurrency for a made-up “client,” and send it to a crypto account they give you. But if you do, the money will be gone, and you’ll be on the hook to repay that money to your bank.

To avoid business, government, and job impersonators, know that

- No legitimate business or government will ever email, text, or message you on social media to ask for money. And they will never demand that you buy or pay with cryptocurrency.
- Never click on a link from an unexpected text, email, or social media message, even if it seems to come from a company you know.
- Don’t pay anyone who contacts you unexpectedly, demanding payment with cryptocurrency.
- Never pay a fee to get a job. If someone asks you to pay upfront for a job or says to buy cryptocurrency as part of your job, it’s a scam.

### Blackmail scams

Scammers might send emails or U.S. mail to your home saying they have embarrassing or compromising photos, videos, or personal information about you. Then, they threaten to make it public unless you pay them in cryptocurrency. Don’t do it. This is blackmail and a criminal extortion attempt. Report it to the [FBI](#) immediately.

## How To Report Cryptocurrency Scams

Report fraud and other suspicious activity involving cryptocurrency to

- the FTC at [ReportFraud.ftc.gov](#)
- the Commodity Futures Trading Commission (CFTC) at [CFTC.gov/complaint](#)
- the U.S. Securities and Exchange Commission (SEC) at [sec.gov/tcr](#)

- the Internet Crime Complaint Center (IC3) at [ic3.gov/Home/FileComplaint](https://ic3.gov/Home/FileComplaint)
- the cryptocurrency exchange company you used to send the money

Search Terms: [business opportunity](#), [cryptocurrency](#), [invest](#), [jobs](#), [scam](#)

Topics: [Jobs and Making Money](#), [Money-Making Opportunities and Investments](#)

Scams: [All Scams](#), [Money-Making Opportunity Scams](#)

May 2022